Host Intrusion Prevention Systems

In the current environment of ever-changing cyber threats, system and network security defenders continue to try and keep pace and limit risk. Proactive (instead of reactive) security measures are becoming a necessity. Among the most effective proactive mitigations is the implementation of a Host Intrusion Prevention System (HIPS).

What is a Host Intrusion Prevention System?

A foundational goal in computer and system security is maintaining the health or integrity of individual hosts — HIPS is a valuable component used to defend computer host integrity. In enterprise deployments, HIPS are centrally managed, and system administrators push policies and rules down to the individual hosts. Alerts of malicious or abnormal activity on the hosts are pushed back up to the management system where they can be correlated and acted upon.

The HIPS policy can be set to log and/or block the malicious or suspicious activity. HIPS generally include four different technologies: a host firewall, a registry monitor, a file integrity monitor, and a process or application behavior monitor.

Host Firewall

Host firewalls place a barrier between the computer and external systems. All information traveling to and sometimes from the computer must pass through the host firewall prior to being fully processed. Ingress firewalls perform stateful inspection and port-blocking on incoming traffic to the host. Typically, only used and necessary ports are left open and unused ports are closed, eliminating the risk of infection through unnecessary ports. An egress firewall will manage which applications are allowed to send data out of the host, usually through a whitelist, thereby reducing the opportunities for exploits and malware to call back to command and control servers. Both inbound and outbound port whitelisting are highly recommended.

Registry Monitor

Most configuration information for a Windows system is found in the registry. The registry stores information about the programs installed, operating system configurations, options to pass to applications as they are invoked, lists of recently executed programs, etc. Registry monitors exist to monitor and protect this crucial part of the Windows operating system. Some monitors take a snapshot and then can be scheduled to run later to compare the current registry settings with the snapshot to identify and alert on unwanted changes. Other monitors try to protect the registry in real-time by intercepting any program trying to make unauthorized changes to the registry.

File Integrity Monitor

Much like the registry monitor, the file integrity monitor reports on changes to critical system and application files. More sophisticated file integrity monitoring can also have the ability to prevent changes to critical system files without user interaction or to roll back altered files to a safer state. In fact, most integrity monitors have the ability to protect both the registry and file system.

Process/Application Behavior Monitor

Process/application behavior monitors study the behavior of processes that are running on the system and alert if an application attempts some action that is outside of its normal or allowed actions. They can also be configured to block this anomalous action. These actions could include accessing the network, writing files to protected directories, writing information to the critical sections of the registry, reading sensitive files, accessing out-of-scope memory, starting new applications, invoking privileged functions, loading untrusted libraries, injecting or hooking other processes, etc.

Considerations

To be effective, it is crucial that a HIPS have a well-defined and tuned policy, or set of rules. Vendors provide many rules with their product, but it is up to the system administrator to tune the rules to their particular environment and to address the specific risks that they face. It is possible that some rules may interfere with business operations. When this happens, create an exception to the rule, refine it until it no longer interferes, or disable it altogether if necessary. To maximize HIPS effectiveness and shorten the amount of time spent deploying HIPS, organizations should work toward a manageable network beforehand. This includes removing/uninstalling unneeded applications, removing/disabling unneeded services, and identifying the source of unusual network traffic.

A useful feature in many HIPS products is the ability to create custom rules. This allows a site to target protections to their particular environment and intellectual property.

Many HIPS products provide the ability to "learn" normal system behavior. This is a double-edged sword. It is convenient because administrators can avoid some of the tedious manual tuning of the HIPS. However, if the learning period coincides with a period when the network is under attack, the HIPS could learn that being attacked is normal and deem that as allowable behavior. Regardless, if the HIPS is set to learning mode, this mode should be disabled after a short period of time so that the HIPS can begin taking action on suspicious activity. Additional manual tuning may be needed.

The importance of dedicated and trained administrators also cannot be overstated. Many rules are passive instead of active; in other words, they are set to alert or log instead of block suspicious activity. Without a trained individual reviewing the logs on a regular basis, no action can be taken to address the suspicious activity. Addressing the anomalous activity includes both investigating machines that are determined to be infected as well as identifying cases where the HIPS rules need to be further tailored to not alert on legitimate activity.

Some commercial examples of HIPS include McAfee's HIPS product (**www.mcafee.com/us/products/host-ips-for-desktop.aspx**) and Symantec's Critical System Protection (**www.symantec.com/critical-system-protection**).

Contact Information

Industry Inquiries: 410-854-6091

USG/IC Client Advocates: 410-854-4790

DoD/Military/COCOM Client Advocates: 410-854-4200

General Inquiries: **niasc@nsa.gov**